

What is claimed is:

1. A digital content protection system that enables a digital content to be used and includes a recording medium apparatus having a storage area for holding digital content information and an access apparatus that reads information from and writes information into the storage area,

the digital content protection system operating according to the following phases:

an authentication phase where the recording medium apparatus secretly transmits an inherent key to the access apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer phase, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the secretly transmitted inherent key.

2. The digital content protection system of Claim 1, wherein the recording medium apparatus includes a first calculation means, and

4 the access apparatus includes a first authentication
5 information generating means and a first authentication
6 means,

7 wherein while the access apparatus judges whether the
8 recording medium apparatus is legitimate in the
9 authentication phase,

10 the first authentication information generating means
11 generates first authentication information and outputs the
12 first authentication information to the recording medium
13 apparatus,

14 the first calculation means receives the first
15 authentication information, generates first calculated
16 authentication information by performing a first calculation
17 on the received first authentication information using the
18 inherent key, and outputs the first calculated authentication
19 information to the access apparatus, and

20 the first authentication means judges whether the
21 recording medium apparatus is legitimate from the first
22 authentication information and the first calculated
23 authentication information using the secretly transmitted
24 inherent key.

1 3. The digital content protection system of Claim 2,
2 wherein the access apparatus includes a second
3 calculation means, and

4 the recording medium apparatus includes a second
5 authentication information generating means and a second
6 authentication means,

7 wherein while the recording medium apparatus judges
8 whether the access apparatus is legitimate in the
9 authentication phase,

10 the second authentication information generating
11 means generates second authentication information and outputs
12 the second authentication information to the access medium
13 apparatus,

14 the second calculation means receives the second
15 authentication information, generates second calculated
16 authentication information by performing a second calculation
17 on the received second authentication information using the
18 secretly transmitted inherent key, and outputs the second
19 calculated authentication information to the recording medium
20 apparatus, and

21 the second authentication means judges whether the
22 access apparatus is legitimate from the second authentication
23 information and the second calculated authentication
24 information using the inherent key.

1 4. The digital content protection system of Claim 3,
2 wherein the recording medium apparatus further
3 includes a first encryption means and an inherent key storing
4 means for prestoring the inherent key, and

5 the access apparatus further includes a first
6 decryption means,

7 wherein while the recording medium apparatus secretly
8 transmits the inherent key to the access apparatus in the
9 authentication phase,

10 the first encryption means generates an encrypted
11 inherent key by applying a first encryption algorithm to the
12 inherent key and outputs the encrypted inherent key to the
13 access apparatus, and

14 the first decryption means receives the encrypted
15 inherent key and generates a decrypted inherent key by
16 applying a first decryption algorithm to the encrypted
17 inherent key, the first decryption algorithm being used to
18 decrypt cipher text generated with the first encryption
19 algorithm.

1 5. The digital content protection system of Claim 4,
2 wherein the recording medium apparatus further
3 includes a first key storing means for prestoring a first
4 key, and

5 the access apparatus further includes a second key
6 storing means for prestoring a second key that corresponds to
7 the first key,

8 wherein the first encryption means encrypts the
9 inherent key using the first key, and

10 the first decryption means decrypts the encrypted
11 inherent key using the second key.

1 6. The digital content protection system of Claim 5,
2 wherein the first key and the second key are the same
3 master key, and

4 the first decryption means decrypts the encrypted
5 inherent key using the second key that is the same as the

6 first key.

1 7. The digital content protection system of Claim 5,
2 wherein the first key is a public key that is
3 calculated from the second key according to a public key
4 determination algorithm of a public key cryptosystem,

5 the first encryption algorithm is an encryption
6 algorithm of the public key cryptosystem, and

7 the first decryption algorithm is a decryption
8 algorithm of the public key cryptosystem,

9 wherein the first encryption means encrypts the
10 inherent key according to the encryption algorithm of the
11 public key cryptosystem using the first key that is the
12 public key, and

13 the first decryption means decrypts the encrypted
14 inherent key according to the decryption algorithm of the
15 public key cryptosystem using the second key.

1 8. The digital content protection system of Claim 5,
2 wherein the second key is a public key that is
3 calculated from the first key according to a public key
4 determination algorithm of a recovery signature processing
5 method,

6 the first encryption algorithm is a signature
7 processing algorithm of the recovery signature processing
8 method,

9 the first encryption means generates the encrypted
10 inherent key that is a signature text by applying the first

11 encryption algorithm to the inherent key using the first
12 key,

13 the first decryption algorithm is a verification
14 processing algorithm of the recovery signature processing
15 method, and

16 the first decryption means generates the decrypted
17 inherent key by applying the first decryption algorithm to
18 the encrypted inherent key that is the signature text using
19 the second key.

1 9. The digital content protection system of Claim 4,
2 wherein the recording medium apparatus further
3 includes:

4 a first master key storing means for prestoring a
5 first master key group that includes a plurality of master
6 keys; and

7 a first selection means for selecting a master key
8 out of the first master key group as a first key, and

9 the access apparatus further includes:

10 a second master key storing means for prestoring a
11 second master key group that includes a plurality of master
12 keys, the first master key group and the second master key
13 group include the same plurality of master keys; and

14 a second selection means for selecting a master key
15 out of the second master key group as a second key, the
16 second key being the same as the first key,

17 wherein the first encryption means encrypts the
18 inherent key using the master key selected as the first key,

19 and
20 the first decryption means decrypts the encrypted
21 inherent key using the master key selected as the second
22 key.

1 10. The digital content protection system of Claim 4,
2 wherein the first encryption means prestores a first
3 subgroup key, generates a transformed key by performing a
4 first conversion on the inherent key using the first subgroup
5 key, and generates the encrypted inherent key by applying the
6 first encryption algorithm to the transformed key, and
7 the first decryption means prestores a second
8 subgroup key that is the same as the first subgroup key,
9 generates a decrypted transformed key by applying the first
10 decryption algorithm to the encrypted inherent key, and
11 generates the decrypted inherent key by performing an
12 inversion operation of the first conversion operation on the
13 decrypted transformed key using the second subgroup key.

1 11. The digital content protection system of Claim 4,
2 wherein the first encryption means prestores a first
3 subgroup key, generates a cipher text by applying the first
4 encryption algorithm to the inherent key, and generates the
5 encrypted inherent key by performing a first conversion
6 operation on the cipher text using the first subgroup key,
7 and
8 the first decryption means prestores a second
9 subgroup key that is the same as the first subgroup key,

generates a decryption text by performing an inverse operation of the first conversion operation on the encrypted inherent key using the second subgroup key, and generates the decrypted inherent key by applying the first decryption algorithm to the decryption text.

12. The digital content protection system of Claim 4, wherein the recording medium apparatus further includes a first key storing means for prestoring a first key that is a master key, and

the access apparatus further includes a second key storing means for prestoring a second key that is the same master key as the first key,

wherein the first encryption means prestores a first subgroup key, generates an encrypted first key by performing a first conversion operation on the first key using the first subgroup key, and generates the encrypted inherent key by applying the first encryption algorithm to the inherent key using the encrypted first key, and

the first decryption means prestores a second subgroup key that is the same as the first subgroup key, generates an encrypted second key by performing a second conversion operation, which is the same as the first conversion operation, on the second key using the second subgroup key, and generates the decrypted inherent key by applying the first decryption algorithm to the encrypted inherent key using the encrypted second key.

1 13. The digital content protection system of Claim 3,
2 wherein the first authentication means includes:
3 a third calculation means for generating third
4 calculated authentication information by performing a third
5 calculation that is the same as the first calculation on the
6 first authentication information using the secretly
7 transmitted inherent key; and

8 a first comparison means for judging whether the
9 first calculated authentication information matches the third
10 calculated authentication information and, if so, determining
11 that the recording medium apparatus is legitimate.

1 14. The digital content protection system of Claim 13,
2 wherein the second authentication means includes:
3 a fourth calculation means for generating fourth
4 calculated authentication information by performing a fourth
5 calculation that is the same as the second calculation on the
6 second authentication information using the inherent key;
7 and

8 a second comparison means for comparing the second
9 calculated authentication information with the fourth
10 calculated authentication information and judging, when the
11 second calculated authentication information matches the
12 fourth calculated authentication information, that the access
13 apparatus is legitimate.

1 15. The digital content protection system of Claim 14,
2 wherein the first calculation means prestores a first

3 subgroup key, generates a transformed inherent key by
4 performing a first conversion operation on the inherent key
5 using the subgroup key, and generates the first calculated
6 authentication information by performing the first
7 calculation on the first authentication information using the
8 transformed inherent key, and

a 9 the third calculation means prestores a second
10 subgroup key that is the same as the first subgroup key,
11 generates a decrypted transformed inherent key by performing
12 an inversion operation of the first conversion operation on
13 the secretly transmitted inherent key using the subgroup key,
14 and generates the third calculated authentication information
15 by performing a calculation that is the same as the first
16 calculation on the first authentication information using the
17 decrypted transformed inherent key.

1 16. The digital content protection system of Claim 14,
2 wherein the first authentication information
3 generating means generates a random number as the first
4 authentication information, and

5 the second authentication information generating
6 means generates a random number as the second authentication
7 information.

1 17. The digital content protection system of Claim 3,
2 wherein the first calculation is a first encryption
3 algorithm,

4 the first calculation means generates the first

5 calculated authentication information by applying the first
6 encryption algorithm to the first authentication information
7 using the inherent key, and

8 the first authentication means generates first
9 decrypted authentication information by applying a first
10 decryption algorithm to the first calculated authentication
11 information using the secretly transmitted inherent key,
12 compares the first authentication information with the first
13 decrypted authentication information, and judges, when the
14 first authentication information matches the first decrypted
15 authentication information, that the recording medium
16 apparatus is legitimate,

17 wherein the first decryption algorithm is used to
18 decrypt a cipher text generated using the first encryption
19 algorithm.

1 18. The digital content protection system of Claim 17,
2 wherein the second calculation is a second encryption
3 algorithm,

4 the second calculation means generates the second
5 calculated authentication information by applying the second
6 encryption algorithm to the second authentication information
7 using the secretly transmitted inherent key, and

8 the second authentication means generates second
9 decrypted authentication information by applying a second
10 decryption algorithm to the second calculated authentication
11 information using the inherent key, compares the second
12 authentication information with the second decrypted

13 authentication information, and judges, when the second
14 authentication information matches the second decrypted
15 authentication information, that the access apparatus is
16 legitimate,

17 wherein the second decryption algorithm is used to
18 decrypt a cipher text generated using the second encryption
19 algorithm.

1 19. The digital content protection system of Claim 18,
2 wherein the first calculation means prestores a first
3 subgroup key, generates a transformed inherent key by
4 performing a first conversion on the inherent key using the
5 first subgroup key, and generates the first calculated
6 authentication information by applying the first encryption
7 algorithm to the first authentication information using the
8 transformed inherent key, and

9 the first authentication means prestores a second
10 subgroup key that is the same as the first subgroup key,
11 generates a decrypted transformed inherent key by performing
12 an inversion operation of the first conversion on the
13 secretly transmitted inherent key using the second subgroup
14 key, and generates the first decrypted authentication
15 information by applying the first decryption algorithm to the
16 first calculated authentication information using the
17 decrypted transformed inherent key.

1 20. The digital content protection system of Claim 18,
2 wherein the first authentication information

3 generating means generates a random number as the first
4 authentication information, and
5 the second authentication information generating
6 means generates a random number as the second authentication
7 information.

a 1 21. The digital content protection system of Claim 3,
2 wherein the storage area holds digital content
3 information that is generated by applying an encryption
4 algorithm to a digital content using the inherent key,

5 the recording medium apparatus further includes an
6 output means for reading, when the recording medium apparatus
7 and the access apparatus have successfully authenticated each
8 other, the digital content information from the storage area
9 and outputting the read digital content information to the
10 access apparatus, and

11 the access apparatus that reads information from the
12 storage area further includes:

13 a content decryption means for receiving the digital
14 content information from the recording medium apparatus and
15 generating a decrypted digital content by applying a
16 decryption algorithm to the digital content information using
17 the secretly transmitted inherent key, the decryption
18 algorithm being used to decrypt a cipher text generated using
19 the encryption algorithm; and

20 a reproduction means for reproducing the decrypted
21 digital content.

0941940-101599

1 22. The digital content protection system of Claim 3,
2 wherein the access apparatus that writes information
3 into the storage area further includes:

4 a content obtaining means for obtaining a digital
5 content from the outside; and

6 a content encryption means for generating digital
7 content information by applying an encryption algorithm to
8 the obtained digital content using the secretly transmitted
9 inherent key, and outputting the digital content information
10 to the recording medium apparatus,

11 wherein the storage area holds the outputted digital
12 content information.

1 23. The digital content protection system of Claim 1,
2 wherein when the recording medium apparatus and the
3 access apparatus have successfully authenticated each
4 other,

5 in the content transfer phase, the access apparatus
6 either

7 (c) generates at least one data block by dividing a
8 digital content, generates a data block key for each data
9 block, generates at least one encrypted data block by
10 encrypting each data block using the secretly transmitted
11 inherent key and a data block key that corresponds to the
12 data block, and transfers each encrypted data block to the
13 recording medium, or

14 (d) receives at least one encrypted data block of an
15 encrypted digital content from the recording medium

16 apparatus, generates a data block key for each data block,
17 and generates at least one data block by decrypting each
18 encrypted data block using the secretly transmitted inherent
19 key and a data block key that corresponds to the encrypted
20 data block,

21 wherein each data block has one of a logical length
22 and a physical length, and

23 each encrypted data block has one of a logical length
24 and a physical length.

1 24. The digital content protection system of Claim 1,
2 wherein when the recording medium apparatus and the
3 access apparatus have successfully authenticated each
4 other,

5 in the content transfer phase, the access apparatus
6 either

7 (e) generates a file key for a file of a digital
8 content, generates an encrypted file by encrypting the file
9 using the secretly transmitted inherent key and the file key,
10 and transfers the encrypted file and information concerning
11 the file key to the recording medium, or

12 (f) receives, from the recording medium apparatus, an
13 encrypted file of an encrypted digital content and
14 information concerning a file key that corresponds to the
15 encrypted file, generates a decrypted file by decrypting the
16 encrypted file using the secretly transmitted inherent key
17 and the information concerning the file key, and reproduces
18 the decrypted file.

1 25. The digital content protection system of Claim 24,
2 wherein when the recording medium apparatus and the
3 access apparatus have successfully authenticated each
4 other,

5 in the content transfer phase, the access apparatus
6 either

7 (g) generates a file key for a file of a digital
8 content, generates an encrypted file by encrypting the file
9 using the file key, generates an encrypted file key by
10 encrypting the file key using the secretly transmitted
11 inherent key, and transfers the encrypted file and the
12 encrypted file key to the recording medium, or

13 (h) receives, from the recording medium apparatus, an
14 encrypted file and an encrypted file key that corresponds to
15 the encrypted file, generates a file key by decrypting the
16 encrypted file key using the secretly transmitted inherent
17 key, generates a decrypted file by decrypting the encrypted
18 file using the file key, and reproduces the decrypted file.

1 26. The digital content protection system of Claim 24,
2 wherein the recording medium apparatus generates a
3 seed from a current time and outputs the seed to the access
4 apparatus, the seed being an initial value of a random
5 number,

6 the access apparatus receives the generated seed from
7 the recording medium apparatus, generates the random number
8 from the seed, and sets the random number as a file key.

27. The digital content protection system of Claim 24,
wherein while the access apparatus judges whether the
recording medium apparatus is legitimate in the
authentication phase,

the access apparatus sends the first authentication
information to the recording medium apparatus,

the recording medium apparatus generates a seed from
a current time, generates a combination result by combining
the seed with the first authentication information, generates
an encrypted combination result by encrypting the combination
result using the inherent key, and sends the encrypted
combination result to the access apparatus, the seed being an
initial value of a random number, and

the access apparatus generates a decrypted seed and
first decrypted authentication information by decrypting the
encrypted combination result using the secretly transmitted
inherent key, judges whether the first authentication
information matches the first decrypted authentication
information, and, if so, determines that the recording medium
apparatus is legitimate, and

in the content transfer phase, the access apparatus
generates the random number from the decrypted seed and sets
the random number as a file key.

28. The digital content protection system of Claim 1,
wherein when the recording medium apparatus and the
access apparatus have successfully authenticated each

other,

in the content transfer phase, the access apparatus either

(i) receives a user key from an operator, generates a transformed key from the user key and the secretly transmitted inherent key, generates an encrypted digital content by encrypting a digital content using the transformed key, and transfers the encrypted digital content to the recording medium, or

(j) receives an encrypted digital content from the recording medium apparatus, generates a transformed key from a user key inputted from an operator and the secretly transmitted inherent key, and generates a decrypted digital content by decrypting the encrypted digital content using the transformed key.

29. The digital content protection system of Claim 1, wherein when the recording medium apparatus and the access apparatus have successfully authenticated each other,

in the content transfer phase, the access apparatus either

(k) receives a user key from an operator, generates a file key for a file of a digital content, generates a transformed key from the user key and the file key, generates an encrypted file by encrypting the file using the transformed key, and transfers the encrypted file and the transformed key to the recording medium, or

13 (1) receives, from the recording medium apparatus, an
14 encrypted file and a transformed key that corresponds to the
15 encrypted file, receives a user key from an operator,
16 generates a file key from the user key and the transformed
17 key, generates a decrypted file by decrypting the encrypted
18 file using the file key, and reproduces the decrypted file.

1 30. The digital content protection system of Claim 1,
2 wherein while the recording medium apparatus judges
3 whether the access apparatus is legitimate in the
4 authentication phase,

5 the recording medium apparatus sends second
6 authentication information to the access apparatus,

7 the access apparatus generates encrypted second
8 authentication information by encrypting the second
9 authentication information using a master key and sends the
10 encrypted second authentication information to the recording
11 medium apparatus, and

12 the recording medium apparatus generates decrypted
13 second authentication information by decrypting the encrypted
14 second authentication information using a master key, judges
15 whether the second authentication information matches the
16 decrypted second authentication information, and, if so,
17 determines that the access apparatus is legitimate.

1 31. The digital content protection system of Claim 1
2 further includes an encrypted inherent key generation
3 apparatus,

4 wherein the digital content protection system further
5 operates according to an encrypted inherent key setting phase
6 where the encrypted inherent key generation apparatus
7 generates an encrypted inherent key by encrypting the
8 inherent key sent from the recording medium apparatus and
9 sends the encrypted inherent key to the recording medium
10 apparatus, and the recording medium apparatus holds the
11 encrypted inherent key sent from the encrypted inherent key
12 generation apparatus,

13 wherein in the authentication phase, the recording
14 medium apparatus sends the encrypted inherent key to the
15 access apparatus, and the access apparatus generates a
16 decrypted inherent key by decrypting the encrypted inherent
17 key secretly sent from the recording medium apparatus and
18 judges whether the recording medium apparatus is legitimate
19 using the decrypted inherent key.

1 32. A recording medium apparatus that has a storage area
2 for holding digital content information and is used in a
3 digital content protection system,

4 wherein the digital content protection system enables
5 a digital content to be used and further includes an access
6 apparatus that reads information from and writes information
7 into the storage area, and

8 the digital content protection system operates
9 according to the following phases:

10 an authentication phase where the recording medium
11 apparatus secretly transmits an inherent key to the access

apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer phase, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the secretly transmitted inherent key.

33. The recording medium apparatus of Claim 32, wherein the recording medium apparatus includes a first calculation means, and

the access apparatus includes a first authentication information generating means and a first authentication means,

wherein while the access apparatus judges whether the recording medium apparatus is legitimate in the authentication phase,

the first authentication information generating means generates first authentication information and outputs the first authentication information to the recording medium apparatus,

the first calculation means receives the first

15 authentication information, generates first calculated
16 authentication information by performing a first calculation
17 on the received first authentication information using the
18 inherent key, and outputs the first calculated authentication
19 information to the access apparatus, and

20 the first authentication means judges whether the
21 recording medium apparatus is legitimate from the first
22 authentication information and the first calculated
23 authentication information using the secretly transmitted
24 inherent key.

1 34. The recording medium apparatus of Claim 33,
2 wherein the access apparatus includes a second
3 calculation means, and

4 the recording medium apparatus includes a second
5 authentication information generating means and a second
6 authentication means,

7 wherein while the recording medium apparatus judges
8 whether the access apparatus is legitimate in the
9 authentication phase,

10 the second authentication information generating
11 means generates second authentication information and outputs
12 the second authentication information to the access medium
13 apparatus,

14 the second calculation means receives the second
15 authentication information, generates second calculated
16 authentication information by performing a second calculation
17 on the received second authentication information using the

09419240-101599

18 secretly transmitted inherent key, and outputs the second
19 calculated authentication information to the recording medium
20 apparatus, and

21 the second authentication means judges whether the
22 access apparatus is legitimate from the second authentication
23 information and the second calculated authentication
24 information using the inherent key.

a 1 35. An access apparatus that reads information from and
2 writes information into a storage area of a recording medium
3 apparatus and is included in a digital content protection
4 system,

5 wherein the storage area holds digital content
6 information,

7 the digital content protection system enables a
8 digital content to be used and includes the recording medium
9 apparatus and the access apparatus,

10 wherein the digital content protection system
11 operates according to the following phases:

12 an authentication phase where the recording medium
13 apparatus secretly transmits an inherent key to the access
14 apparatus, and the recording medium apparatus and the access
15 apparatus perform mutual authentication using the inherent
16 key, the inherent key being information that is unique to the
17 recording medium apparatus; and

18 a content transfer phase, performed only when the
19 recording medium apparatus and the access apparatus have
20 successfully authenticated each other, where the access

21 apparatus either (a) encrypts a digital content using the
22 secretly transmitted inherent key and sends the encrypted
23 digital content to the recording medium apparatus or (b)
24 receives an encrypted digital content from the recording
25 medium apparatus and decrypts the encrypted digital content
26 using the secretly transmitted inherent key.

1 36. The access apparatus of Claim 35,
2 wherein the recording medium apparatus includes a
3 first calculation means, and

4 the access apparatus includes a first authentication
5 information generating means and a first authentication
6 means,

7 wherein while the access apparatus judges whether the
8 recording medium apparatus is legitimate in the
9 authentication phase,

10 the first authentication information generating means
11 generates first authentication information and outputs the
12 first authentication information to the recording medium
13 apparatus,

14 the first calculation means receives the first
15 authentication information, generates first calculated
16 authentication information by performing a first calculation
17 on the received first authentication information using the
18 inherent key, and outputs the first calculated authentication
19 information to the access apparatus, and

20 the first authentication means judges whether the
21 recording medium apparatus is legitimate from the first

22 authentication information and the first calculated
23 authentication information using the secretly transmitted
24 inherent key.

1 37. The access apparatus of Claim 36,

2 wherein the access apparatus includes a second
3 calculation means, and

4 the recording medium apparatus includes a second
5 authentication information generating means and a second
6 authentication means,

7 wherein while the recording medium apparatus judges
8 whether the access apparatus is legitimate in the
9 authentication phase,

10 the second authentication information generating
11 means generates second authentication information and outputs
12 the second authentication information to the access medium
13 apparatus,

14 the second calculation means receives the second
15 authentication information, generates second calculated
16 authentication information by performing a second calculation
17 on the received second authentication information using the
18 secretly transmitted inherent key, and outputs the second
19 calculated authentication information to the recording medium
20 apparatus, and

21 the second authentication means judges whether the
22 access apparatus is legitimate from the second authentication
23 information and the second calculated authentication
24 information using the inherent key.

1 38. An encrypted inherent key generating apparatus that
2 is used in a digital content protection system,

3 wherein the digital content protection system that
4 enables a digital content to be used and includes a recording
5 medium apparatus having a storage area for holding digital
6 content information and an access apparatus that reads
7 information from and writes information into the storage
8 area,

9 the digital content protection system operating
10 according to the following phases:

11 an encrypted inherent key setting phase where the
12 encrypted inherent key generation apparatus generates an
13 encrypted inherent key by encrypting the inherent key sent
14 from the recording medium apparatus and sends the encrypted
15 inherent key to the recording medium apparatus, and the
16 recording medium apparatus holds the encrypted inherent key
17 sent from the encrypted inherent key generation apparatus,
18 wherein the inherent key is information that is unique to the
19 recording medium apparatus;

20 an authentication phase where the recording medium
21 apparatus transmits the encrypted inherent key to the access
22 apparatus, the access apparatus generates an decrypted
23 inherent key by decrypting the encrypted inherent key
24 transmitted from the recording medium apparatus, the
25 recording medium apparatus judges whether the access
26 apparatus is an authorized apparatus using the inherent key,
27 and the access apparatus judges whether the recording medium

a

005107-0426TH60

28 apparatus is an authorized apparatus using the decrypted
29 inherent key; and

30 a content transfer phase, performed only when the
31 recording medium apparatus and the access apparatus have
32 successfully authenticated each other, where the access
33 apparatus either (a) encrypts a digital content using the
34 decrypted inherent key and sends the encrypted digital
35 content to the recording medium apparatus or (b) receives an
36 encrypted digital content from the recording medium apparatus
37 and decrypts the encrypted digital content using the
38 decrypted inherent key.

1 39. A digital content protection method used in a digital
2 content protection system that enables a digital content to
3 be used and includes a recording medium apparatus having a
4 storage area for holding digital content information and an
5 access apparatus that reads information from and writes
6 information into the storage area,

7 the digital content protection method comprising:
8 an authentication step where the recording medium
9 apparatus secretly transmits an inherent key to the access
10 apparatus, and the recording medium apparatus and the access
11 apparatus perform mutual authentication using the inherent
12 key, the inherent key being information that is unique to the
13 recording medium apparatus; and

14 a content transfer step, performed only when the
15 recording medium apparatus and the access apparatus have
16 successfully authenticated each other, where the access

apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the secretly transmitted inherent key.

40. A digital content protection program that is recorded on a computer-readable recording medium and is executed in a digital content protection system,

wherein the digital content protection system enables a digital content to be used and includes a recording medium apparatus having a storage area for holding digital content information and an access apparatus that reads information from and writes information into the storage area,

the digital content protection program comprising:

an authentication step where the recording medium apparatus secretly transmits an inherent key to the access apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer step, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b)

22 receives an encrypted digital content from the recording
23 medium apparatus and decrypts the encrypted digital content
24 using the secretly transmitted inherent key.

1 41. A computer digital signal that is sent via a
2 communication channel and includes a digital content
3 protection program used in a digital content protection
4 system,

5 wherein the digital content protection system enables
6 a digital content to be used and includes a recording medium
7 apparatus having a storage area for holding digital content
8 information and an access apparatus that reads information
9 from and writes information into the storage area,

10 the digital content protection program comprising:

11 an authentication step where the recording medium
12 apparatus secretly transmits an inherent key to the access
13 apparatus, and the recording medium apparatus and the access
14 apparatus perform mutual authentication using the inherent
15 key, the inherent key being information that is unique to the
16 recording medium apparatus; and

17 a content transfer step, performed only when the
18 recording medium apparatus and the access apparatus have
19 successfully authenticated each other, where the access
20 apparatus either (a) encrypts a digital content using the
21 secretly transmitted inherent key and sends the encrypted
22 digital content to the recording medium apparatus or (b)
23 receives an encrypted digital content from the recording
24 medium apparatus and decrypts the encrypted digital content

a

25 using the secretly transmitted inherent key.

09449240-1059
665707 04267460